

SECUENCIA DIDACTICA: CRIPTOGRAFÍA

JUSTIFICACIÓN

Esta dirigida a alumnos de 2º de ciclo medio de informática, del Módulo “Seguridad Informática”. La voy a llevar a cabo en 10 sesiones, de las cuales 4 van a ser teóricas y 6 prácticas.

Se trata de estudiar los métodos y herramientas para asegurar la privacidad de la información transmitida entre ordenadores. Pretendo que describan e identifiquen sistemas lógicos de identificación y utilizar sistemas de identificación lógica como la firma electrónica o el certificado digital.

Las Unidades de Competencia van a ser:

- Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos (UCO 959_2).
- Mantener y regular el subsistema físico en sistemas informáticos (UCO 957_2)

OBJETIVOS GENERALES

- Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático.
- Asegurar la privacidad de la información transmitida por redes informáticas, describir vulnerabilidades e instalar software específico.
- Extraer información general y específica de textos en L2
- Conocer y comprender conceptos y expresiones en L2

CONTENIDOS

Los contenidos se valorarán en función de los conceptos adquiridos, los procedimientos aprendidos y las actitudes desarrolladas en las clases.

Conceptos

- Métodos para asegurar la privacidad de la información transmitida
- Conceptos y Expresiones en L2
- Criptografía
 - Cifrado de clave secreta (simétrica)
 - Cifrado de clave pública (asimétrica)

- Funciones de mezcla o resumen (hash)
- Sistemas de identificación
 - Firma digital
 - Certificados digitales
 - Distribución de claves. PKI
 - Tarjetas inteligentes
- Seguridad del sistema
 - Amenazas y ataques
 - Seguridad en el arranque
 - Particiones del disco y seguridad
 - Actualizaciones y parches de seguridad en el sistema y en las aplicaciones
 - Autenticación de usuarios
 - Listas de control de acceso
 - Sistemas biométricos
 - Política de contraseñas
 - Cuotas de disco
 - Monitorización y logs del sistema
- Software que vulnera la seguridad del sistema
 - Clasificación de atacantes
 - Tipos de ataques (sniffing, DoS, virus, etcetera)
 - Software malicioso (malware)
 - Técnicas usadas para el fraude y robo (ingeniería social, phishing, spoofing, etcétera)
 - Impactos
 - Educación y formación del usuario. Consejos prácticos. Copias de seguridad e imágenes de respaldo

Procedimientos

- Cifrar textos mediante diversos algoritmos.
- Generar parejas de claves para el cifrado asimétrico.
- Exportar e importar certificados.
- Intercambiar claves o certificados.
- Revocar un certificado.
- Instalar una entidad emisora de certificados.
- Realizar peticiones de certificados a una entidad emisora.
- Retirar certificados.
- Firmar mensajes.
- Obtener certificados digitales.
- Enviar correos electrónicos haciendo uso del certificado digital en L2

C. Actitudes

- Apreciar la necesidad de cifrar la información para mantener la confidencialidad.
- Valorar la importancia del uso de los certificados y firmas digitales.
- Mostrar interés en la adquisición de los conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos en L2

ACTIVIDADES

-Introducción de la teoría en L1 y L2.

-Aplicar mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático:

- inventar un modelo de cifrado simétrico para comunicarse de manera segura con un compañero. Describir sus características (L2)
- describir las características del morse como método de cifrado (L2).

-Cifrar mediante el algoritmo del César la frase: “El gran avance de la criptografía tuvo lugar durante el siglo xx” utilizando L2.

-Asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico

- cifrar un documento en L2 utilizando la aplicación pgp.
- mediante la misma aplicación envía mensajes cifrados a tus compañeros y descifra los recibidos
- indicar en L2 que trámites puedes realizar con el certificado digital

-investigar lo que contiene en su chip el DNI electrónico, para ello entra en la página web del portal oficial sobre el DNI electrónico:http://www.dnielectronico.es/Guia_Basica/descrip_fisica.html. Hacer un breve resumen en L2

METODOLOGÍA

Dado que los alumnos de ciclo vienen de una formación general, es fundamental conectar tantas veces como sea posible los conceptos explicados con situaciones prácticas y cercanas a la realidad laboral. Por este motivo, las actividades propuestas se han basado en tareas que se realizan habitualmente en el mundo profesional.

Uno de los objetivos de la enseñanza en formación profesional es capacitar a los alumnos para que sepan trabajar de manera independiente. Por este motivo, las actividades deben capacitar a que los alumnos avancen por sí mismos en su propio proceso de aprendizaje.

El que se facilite el aprendizaje independiente no es óbice para que muchas de las situaciones del proceso de enseñanza aprendizaje se planteen trabajarlas de manera cooperativa.

CRITERIOS DE EVALUACIÓN

Los requisitos mínimos para superar esta unidad pasan, a nivel más concreto, por el aprendizaje de los siguientes conceptos:

- Instalar, probar y actualizar aplicaciones específicas para la detección y eliminación de software malicioso.
- Describir y utilizar sistemas lógicos de identificación como la firma electrónica, el certificado digital, etcétera.
- Valorar las ventajas que supone la utilización de sistemas biométricos.
- Clasificar y detectar las principales incidencias y amenazas lógicas de un subsistema lógico.
- Aplicar técnicas de monitorización de accesos y actividad e identificar situaciones anómalas.
- Utilizar la L2

